





Efficient Asymmetric PAKE Compiler from KEM and AE

You Lyu^{1,2}, Shengli Liu^{1,2}, and Shuai Han^{2,3}

¹ Department of Computer Science and Engineering
Shanghai Jiao Tong University, Shanghai 200240, China

² State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

³ School of Cyber Science and Engineering, Shanghai Jiao Tong University,
Shanghai 200240, China

{`vergil, slliu, dalen17`}@sjtu.edu.cn

Abstract. Password Authenticated Key Exchange (PAKE) allows two parties to establish a secure session key with a shared low-entropy password pw . Asymmetric PAKE (aPAKE) extends PAKE in the client-server setting, and the server only stores a password file instead of the plain password so as to provide additional security guarantee when the server is compromised.

In this paper, we propose a novel generic compiler from PAKE to aPAKE in the Universal Composable (UC) framework by making use of Key Encapsulation Mechanism (KEM) and Authenticated Encryption (AE).

- Our compiler admits efficient instantiations from lattice to yield lattice-based post-quantum secure aPAKE protocols. When instantiated with Kyber (the standardized KEM algorithm by the NIST), the performances of our compiler outperform other lattice-based compilers (Gentry et al. CRYPTO 2006) in all aspects, hence yielding the most efficient aPAKE compiler from lattice. In particular, when applying our compiler to the UC-secure PAKE schemes (Santos et al. EUROCRYPT 2023, Beguinet et al. ACNS 2023), we obtain the most efficient UC-secure aPAKE schemes from lattice.
- Moreover, the instantiation of our compiler from the tightly-secure matrix DDH (MDDH)-based KEM (Pan et al. CRYPTO 2023) can compile the tightly-secure PAKE scheme (Liu et al. PKC 2023) to a tightly-secure MDDH-based aPAKE, which serves as the first tightly UC-secure aPAKE scheme.

Keywords: Password authenticated key exchange; asymmetric password authenticated key exchange; lattice; post-quantum security

1 Introduction

Password Authenticated Key Exchange (PAKE) facilitates a secure establishment of session keys between two parties, say a client and a server, over a public